1 **What is claimed:**

2

1 1.   An improved method for encryption, comprising:

2   receiving original data to be encrypted;

3   performing cipher steps to process the original data into encrypted data,

4 including:

5   looking up logs of terms being multiplied over a finite field;

6   summing the logs to obtain a sum; and

7   looking up the anti-log of the sum;

8   outputting the encrypted data.

9

1 2.   The method of Claim 1, wherein looking up the log of terms comprises looking up

2 the log of terms in a primitive power and log table.

3

1 3.   The method of Claim 2, wherein looking up the anti-log of the sum comprises

2 looking up the anti-log of the sum in the primitive power and log table.

3

1 4.   The method of Claim 2, wherein:

2   the finite field is a Galois field; and

3   looking up the log of terms in a primitive power and log table comprises looking

4 up the log of terms in a primitive power and log table, of a primitive element of the

5 Galois field.

6

1 5.   The method of Claim 1, wherein:

2   the encryption utilizes the AES algorithm, wherein the AES algorithm includes a

3 Cipher and an Inverse Cipher, and wherein the Cipher includes a MixColumns

4 transform, and wherein the Inverse Cipher includes an InvMixColumns transform; and

5   looking up the log of terms being multiplied comprises looking up the logs of

6 terms being multiplied over a finite field in the MixColumns transform of the Cipher and

10

7   in the InvMixColumns transform of the Inverse Cipher.

8

1   6.   The method of Claim 5, wherein looking up the logs of terms being multiplied

2   over a finite field in the MixColumns transform of the Cipher and in the InvMixColumns

3   transform of the Inverse Cipher comprises looking up the logs of terms being multiplied

4   over a Galois field in the MixColumns transform of the Cipher and in the InvMixColumns

5   transform of the Inverse Cipher.

6

1   7.   The method of Claim 1, wherein looking up the log of terms being multiplied over

2   a finite field comprises looking up the log of terms being multiplied over a Galois field.

3

1   8.   The method of Claim 1, wherein looking up the log of terms comprises looking up

2   the log of terms in a table comprising 2 rows.

3

1   9.   The method of Claim 1, further including:

2   transmitting the encrypted data:

3   receiving the encrypted data;

4   performing Inverse Cipher steps including:

5   looking up the log of terms being multiplied over the finite field;

6   summing the logs to obtain a sum;

7   looking up the anti-log of the sum; and

8   outputting the original data.

9

1   10.   An encryption system comprising:

2   a first communications device adapted to receive original data and including:

3   means for encrypting the original data to generate encrypted data,

4   including:

5   means for performing a MixColumns transform including:

6   means for looking up logs of terms being multiplied over a finite

11

7   field;

8   means for summing the logs to obtain a sum;

9   means for looking up the anti-log of the sum; and

10   means for outputting the encrypted data.

11

1   11.   The system of Claim 10, wherein the means for encrypting the original data

2   comprises a processor adapted to exercise the AES algorithm.

3

1   12.   The system of Claim 10, wherein the finite field is a Galois filed (2^8).

2

1   13.   An inverse encryption system comprising:

2   a second communications device adapted to receive encrypted data, and

3   including:

4   means for inverse encrypting the encrypted data to generate original data,

5   including:

6   means for performing an InvMixColumns transform including:

7   means for looking up logs of terms being multiplied over a

8   finite field;

9   means for summing the logs to obtain a sum;

10   means for looking up the anti-log of the sum; and

11   means for outputting the original data.

12

1   14.   The system of Claim 13, wherein the means for encrypting the original data

2   comprises a processor adapted to exercise the AES algorithm.

1

2   15.   The system of Claim 13, wherein the finite field is a Galois filed (2^8).

1

2   16.   An improved method for encryption including multiplication over a finite field, the

3   improvement comprising:

4   obtaining the result of multiplication over the finite field using a primitive power

5 and log table comprising 2 rows.

6

1   17.   The method of Claim 16, wherein obtaining the result of multiplication over a

2 finite field comprises:

3   looking up logs of terms being multiplied over the finite field;

4   summing the logs to obtain a sum; and

5   looking up the anti-log of the sum.

6

1   18.   The method of Claim 16, wherein obtaining the result of multiplication over a

2 finite field comprises obtaining the result of multiplication over a Galois field(2^8)

3 performed in the MixColumns transformation and in the InvMixColumns transformation

4 of the AES algorithm, using a 2 by 256 primitive power and log table, comprising the

5 steps of:

6   looking up logs of terms being multiplied over the Galois field(2^8);

7   summing the logs to obtain a sum; and

8   looking up the anti-log of the sum.

9

1   19.   The improvement of Claim 16, wherein the primitive power and log table is based

2 on a primitive is selected from the set consisting of the 128 primitives of the Galois

3 field(2^8).

4

1   20.   The improvement of Claim 16, wherein the improvement is implemented in C

2 code.

3

1   21.   The improvement of Claim 16, wherein the improvement is implemented in

2 assembly code in a Digital Signal Processing (DSP) chip.

3

13